



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/629,104	07/29/2003	Jian Huang	CM03751J	6368
24131	7590	12/29/2006	EXAMINER	
LERNER GREENBERG STEMER LLP P O BOX 2480 HOLLYWOOD, FL 33022-2480			GELAGAY, SHEWAYE	
		ART UNIT	PAPER NUMBER	
		2137		
SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE		
3 MONTHS	12/29/2006	PAPER		

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>	
	10/629,104	HUANG ET AL.	
	<b>Examiner</b>	<b>Art Unit</b>	
	Shewaye Gelagay	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) Responsive to communication(s) filed on 29 July 2003.  
 2a) This action is FINAL.                    2b) This action is non-final.  
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) Claim(s) 1-49 is/are pending in the application.  
 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.  
 5) Claim(s) \_\_\_\_\_ is/are allowed.  
 6) Claim(s) 1-26 and 33-49 is/are rejected.  
 7) Claim(s) 27-32 is/are objected to.  
 8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) The specification is objected to by the Examiner.  
 10) The drawing(s) filed on \_\_\_\_\_ is/are: a) accepted or b) objected to by the Examiner.  
     Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
     Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).  
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
 a) All    b) Some \* c) None of:  
     1. Certified copies of the priority documents have been received.  
     2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
     3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)            | 4) <input type="checkbox"/> Interview Summary (PTO-413)           |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)   | Paper No(s)/Mail Date: _____                                      |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date <u>7/29/03</u> .   | 6) <input type="checkbox"/> Other: _____                          |

## DETAILED ACTION

1. Claims 1-49 have been examined.

### ***Claim Rejections - 35 USC § 103***

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 1-26 and 33-49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Zheng et al. (hereinafter Zheng) in view of Law et al. "Key Management with Group-Wise Pre-Deployed Keying and Secret Sharing Pre-Deployed Keying" (hereinafter Law) and in view of Laroia et al. (hereinafter Laroia) US Patent Number 6,961,595.

As per claims 1 and 46-49:

Zheng teaches a method for secured software patching and upgrade in a distributed wireless sensor network, which comprises:

providing a spanning-tree network of communications nodes with at least one root, node and at least one software upgrade repository; (page 9, paragraph 140)  
receiving a software upgrade with the root node; (page 6, paragraphs 88-89)  
communicating the upgrade from the root node to the software upgrade repository; (page 6, paragraphs 88-89 and 96) and

delivering and installing the upgrade in the software upgrade repository after authentication occurs. (page 6, paragraphs 88-89 and 95-96)

upgrade in the same upgrade session and forming, with the nodes in the same session, a group with a unique group session key determined by the software upgrade repository and maintaining the session key with the software upgrade repository; (page 12, paragraph 174)

installing the upgrade on the software upgrade repository by:

exchanging at least one of a key length, a session key, a patch key, and a prime modulus between the two nodes undertaking the upgrade and sharing the session key and the prime modulus with all of the nodes in the same session; (page 9, paragraph 133; page 11, paragraphs 163-164)

authenticating a patch key and delivering and installing the upgrade in the software upgrade repository after authentication occurs; (page 9, paragraph 133; page 11, paragraphs 163-164) and

starting the software upgrade installation from the software upgrade repository along a respective branch and repeating the software upgrade installation through the branch until all leaf nodes on the branch have the upgrade installed thereon. (page 6, paragraphs 88-89 and 95-96)

Zheng does not explicitly teach generating patch keys locally on each node according to the Diffie-Hellman algorithm; and carrying out the installation of the upgrade in parallel on orthogonal branches of the network. Law in analogous art, however, discloses generating patch keys locally on each node according to the Diffie-

Hellman algorithm. (page 2, section 4) Therefore, it would have been obvious to one ordinary skill in the art at the time the invention was made to modify the method disclosed by Zheng with Law in order to reduce the secret from being divulged to untrusted nodes by using implementing a system that makes use of shared key without reconstructing the key itself. (page 2, section 4; Law)

Both references do not explicitly disclose carrying out the installation of the upgrade in parallel on orthogonal branches of the network. Laroia in analogous art, however, discloses carrying out the installation of the upgrade in parallel on orthogonal branches of the network. (col. 4, lines 44-51) Therefore, it would have been obvious to one ordinary skill in the art at the time the invention was made to modify the method disclosed by Zheng and Law with Laroia in order to avoid interference from transmission signals generated by multiple nodes in the same cell (col. 4, lines 49-51; Laroia)

As per claim 2:

The combination of Zheng, Law and Laroia teaches all the subject matter as discussed above. In addition, Zheng further discloses a method which comprises providing the communications nodes as sensor devices each sensing, processing, transmitting, receiving, and actuating in a given geographical area. (page 1, paragraph 9)

As per claim 3:

The combination of Zheng, Law and Laroia teaches all the subject matter as discussed above. In addition, Zheng further discloses a method comprises: deploying and managing the patch key of the software upgrade repository with the root node; and

defining a length of the patch key with the root node. (page 6, paragraphs 88-89 and 96)

As per claims 4 and 39:

The combination of Zheng, Law and Laroia teaches all the subject matter as discussed above. In addition, Zheng further discloses a method carrying out subgroup controller functions with the software upgrade repository; coordinating new patch key deployment with the software upgrade repository; and managing all of the nodes underneath the software upgrade repository on the same branch of the spanning tree with the software upgrade repository. (page 6, paragraphs 88-89 and 96)

As per claim 5:

The combination of Zheng, Law and Laroia teaches all the subject matter as discussed above. In addition, Zheng further discloses a method varying a length of the patch key on at least one branch of the spanning-tree. (page 9, paragraph 140)

As per claims 6-8:

The combination of Zheng, Law and Laroia teaches all the subject matter as discussed above. In addition, Zheng further discloses a method providing at least one root node of the network as a gateway to another network. (page 9, paragraph 140)

As per claim 9:

The combination of Zheng, Law and Laroia teaches all the subject matter as discussed above. In addition, Zheng further discloses a method carrying out the installation of the upgrade in parallel on a plurality of software upgrade repositories within the same upgrade session. (page 12, paragraph 174)

As per claim 10:

Art Unit: 2137

The combination of Zheng, Law and Laroia teaches all the subject matter as discussed above. In addition, Laroia further discloses a method carrying out the installation of the upgrade in parallel on orthogonal branches of the network. (col. 4, lines 44-51)

As per claims 11 and 25:

The combination of Zheng, Law and Laroia teaches all the subject matter as discussed above. In addition, Laroia further discloses a method carrying out the installation of the upgrade in parallel on orthogonal branches of the network within the same upgrade session. (col. 4, lines 44-51)

As per claims 12-13 and 15-17:

The combination of Zheng, Law and Laroia teaches all the subject matter as discussed above. In addition, Zheng further discloses a method forming, with the nodes in the same session, a group with a unique group session key determined by the software upgrade repository. (page 12, paragraph 174)

As per claims 14 and 18:

The combination of Zheng, Law and Laroia teaches all the subject matter as discussed above. In addition, Law further discloses a method generating a two-byte patch key with the Diffie-Hellman algorithm in every step along the branch on each node in the same session. (page 2, section 4)

As per claim 19:

The combination of Zheng, Law and Laroia teaches all the subject matter as discussed above. In addition, Zheng further discloses a method carrying out the

authentication with variable-length patch keys having a given length for the software upgrade repository and a shorter length for nodes of the network farther away from the root node than the software upgrade repository. (page 12, paragraph 174)

As per claims 20-21, 26 and 40-41:

The combination of Zheng, Law and Laroia teaches all the subject matter as discussed above. In addition, Zheng further discloses a method carrying out the authentication with different length patch keys, a patch key having a given length for communications between the root node and the software upgrade repository and another patch key having a length shorter than the given length for communications between the software upgrade repository and nodes farther away from the root node than the at least one software upgrade repository. (page 9, paragraph 133; page 11, paragraphs 163-164; page 12, paragraph 174)

As per claim 22-23 :

The combination of Zheng, Law and Laroia teaches all the subject matter as discussed above. In addition, Zheng further discloses a method defining the software upgrade repository to be immediate children of the root node; and managing the software upgrade repository with the root node. (page 9, paragraph 133; page 11, paragraphs 163-164; page 12, paragraph 174)

As per claim 24:

The combination of Zheng, Law and Laroia teaches all the subject matter as discussed above. In addition, Law further discloses a method carrying out the authentication with patch keys generated locally on each node according to the Diffie-

Art Unit: 2137

Hellman algorithm. (page 2, section 4)

As per claims 33, 38 and 42:

The combination of Zheng, Law and Laroia teaches all the subject matter as discussed above. In addition, Zheng further discloses a method carrying out the upgrade installation by: downloading at least one upgrade from an upgrade server and saving the upgrade on a device in the network to be upgraded including at least one of the root node, the software upgrade repository, and a node; sending information regarding present characteristics of the device to be upgraded to the upgrade server and determining, with the upgrade server, if an upgrade needs to be performed for the device; receiving, with the device to be upgraded, a response to the information sent from the upgrade server and parsing the response to determine what aspects of the device needs to be upgraded; selecting an appropriate upgrade with the device to be upgraded, sending a request to the upgrade server to send the appropriate upgrade, and downloading relevant upgrade data; and saving the upgrade data in the device at a temporary storage sector. (page 6, paragraph 96)

As per claims 34-37:

The combination of Zheng, Law and Laroia teaches all the subject matter as discussed above. In addition, Zheng further discloses a method providing the upgrade server as any device in the network able to transfer the upgrade. (page 6, paragraph 96)

As per claims 38 and 43-45:

The combination of Zheng; Law and Laroia teaches all the subject matter as discussed above. In addition, Zheng further discloses a method carrying out the upgrade installation by: switching a node in the network to an upgrade mode at a given time; and switching the node to a working mode if the temporary storage sector is empty and, if the temporary storage sector is not empty: determining from the upgrade data in the temporary storage sector a destination sector number in software of the device for the upgrade; and writing the upgrade data from the temporary storage sector over a data section of the destination sector in the software of the device.

***Allowable Subject Matter***

4. Claim 27 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

The following is a statement of reasons for the indication of allowable subject matter: None of the prior art on the record specifically teaches a method which further comprises generating and exchanging the patch key and prime modulus by: first, generating the patch key with the software upgrade repository utilizing the key length, a secret key, and a predefined prime modulus; second, executing the Diffie-Helman algorithm with the software upgrade repository to obtain the patch key; third, sending at least the key length, the patch key, and the prime modulus, to the node to be upgraded; fourth, picking a random secret number and executing the Diffie-Heilman algorithm with the node to be upgraded to generate a patch key of the node, and sending the patch

key of the node to the software upgrade repository; fifth, authenticating correct reception of the patch key of the node as a condition for the software upgrade repository to authenticate a session key back to the node; sixth, executing the Diffie-Hellman algorithm with the software upgrade repository upon receiving the patch key of the node to generate a session key; seventh, authenticating the node to proceed and start the upgrade installation on the node when the node receives the session key.

5. Claims 28-32, which are directly or indirectly dependents of claim 25 are also objected.

***Conclusion***

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See Form PTO-892.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shewaye Gelagay whose telephone number is 571-272-4219. The examiner can normally be reached on 8:00 am to 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2137

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Shewaye Gelagay

Cynthia Britt  
12-20-06  
AU 2138

Cynthia Britt  
Preliminary EXAMINER